In “New Attack Tricks Antivirus Software,” Karen Heyman outlines the new threats of malware (as of 2007). Heyman first describes DCO, or dynamic code obfuscation. Essentially, it hides and constantly changes the virus code through obfuscation and polymorphism to keep any antivirus software from recognizing it as malware to slip behind security, but still has a high level of danger when an attack succeeds. Through JavaScript, any person viewing the browser can access the code used to create the browser, and hackers can utilize this to identify places where their virus can embed itself for others to access on their machines. DCO traps include spam or phishing that may lure a person to a seemingly normal website which when interacted with, releases the virus onto the machine, or may release the virus onto the machine directly from an email.

Getting into more specifics about how DCO works, the process is such that the hacker’s website with break up or change the JavaScript code before a victim attempts to download it so that the antivirus software will not recognize it as malicious, and then a subroutine within the code allows it to be put back together and execute on the victim’s machine. Meanwhile, the original code is kept and maintained on the hacker’s website to be changed again for the next victim so that no two victims receive the exact same JavaScript code. New antivirus techniques will include assessing the safety of the browser itself, behavioral matching (what does the program do once downloaded?), and pattern analyzing to decode the obfuscated code and then analyze what the code is meant to do before letting it execute.

What interests me about this article is that the last article I read (“Worm Epidemics”) was only three years prior, and yet the level of hacking techniques seems exponentially greater. Then, I wonder about the fact that this article was written in 2007, which is fourteen years ago from the present day, and how different malware tactics might be today. However, with Webroot Threat Shield as an extension on my Google Chrome browser, I think I have successfully avoided any malicious software attacks, so luckily it seems that the defense against malicious software has also matured exceptionally well.